



Privacy and Data Governance

New requirements and opportunities

JANUARY 2022

New requirements for protecting personal information

After more than a year of discussions and parliamentary proceedings regarding Bill 64, the *Act to modernize legislative provisions as regards the protection of personal information* was adopted on September 21, 2021 (SQ 2021, c 25) (hereinafter the “Act”), significantly amending the rules for the protection and processing of personal information (PI) that must be followed by any organization or business that collects, processes or holds personal information in Québec.

The initial modifications take effect on September 22, 2022 while the remaining ones will be effective in September 2023 and 2024.

What, more specifically, are these new requirements?

The Act imposes new obligations, sets out various requirements, grants new rights and imposes safeguards to manage risk for projects and solutions that involve processing PI, disclosing PI to third parties and outsourcing. It also recommends transparency throughout the entire life cycle of PI. In addition, the Act grants more power to the regulatory authority. The new requirements constitute a reform similar to the one resulting from the General Data Protection Regulation (GDPR).

We describe here the business requirements resulting from the changes brought about by the Act and will offer support to businesses to help them move towards digitization and upgrade their privacy protection and data management program.

A good opportunity

The amendments resulting from the coming into force of the Act require that significant changes be made to the processes and practices that involve PI processing. These required changes are also a good opportunity to review and optimize data governance, which includes regulatory compliance.

In addition to the regulatory requirements, the **Act provides a good opportunity to take control of data and leverage this strategic asset**, making it possible to:

-
- **Implement a transparent client- and employee-centric approach:** the primary objective of the Act is to protect the rights and interests of your clients and employees. Requirements relating to consent and people's rights will make it possible to clearly indicate the measures put in place to protect the personal information of clients and employees, thereby strengthening trust;
-
- **Improve security:** implementing the requirements of the Act will help improve your organization's overall information security posture;
-
- **Develop your data management capabilities:** by taking back control, you will have a better grasp of your data and increase your capability to leverage this strategic asset;
-
- **Accelerate digitization:** data is at the heart of digital transformation. The new requirements make it possible to put in place the basis for good governance and data management, which helps to accelerate digitization;
-
- **Put in place a strategy for obtaining and managing consent** that brings you closer to your clients and employees, allowing you to better meet their needs with a management approach that focusses on their preferences.
-

A holistic approach

KPMG prefers to take a pragmatic, holistic approach that is based on complementary skills and collaboration with data professionals in matters pertaining to cybersecurity, privacy, data governance, automation, document management, digital transformation, identity and access management, customer experience (“CX”) and change management.

The approach should be consistent with the existing management framework and seek to:

-
- Organize data governance by establishing:
 - A target operating model;
 - People’s roles and responsibilities;
 - Policies and rules for managing and protecting data;
 - Measures for monitoring progress and improvements.
-
- Develop a consent management strategy that is well thought out and integrated into the customer journey;
-
- Classify and categorize data and information assets to identify and map personal information;
-
- Review security policies and strengthen processes for managing incidents, access and controls;
-
- Build team awareness, train your employees and provide support for these key organizational changes.
-

KPMG has complementary, multidisciplinary advisory capabilities to support businesses as they endeavour to ensure compliance for privacy, data governance and the implementation of solid consent management strategies.

Contact us!



Jean-François De Rico

Lead Partner,
Data Privacy
KPMG in Canada

jderico@kpmg.ca

418 577-3442



Catherine Nadeau

Senior Manager,
Data Governance
KPMG in Canada

cnadeau@kpmg.ca

514 840-5350



Meeting the new requirements

An approach that seeks to strengthen compliance with the new requirements must be based on the following major areas:

APPROACH FOR STRENGTHENING COMPLIANCE

- Assess the current situation
- Determine target and risk appetite
- Analyze discrepancies between current situation and compliance target
- Determine and prioritize action plans (roadmap)
- Choose technological solutions
- Oversee implementation, change management, awareness/training

Below is a list of the requirements stemming from the new requirements, based on their impact on governance, processes, technology and human resources:

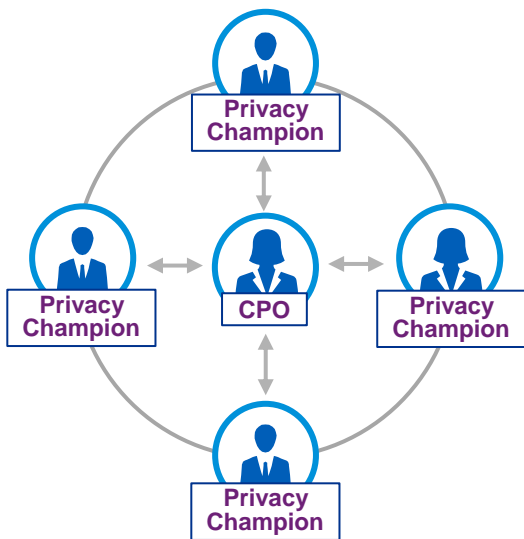
- Roles and responsibilities
- Policies, processes and solutions
- Impact assessment
- Collection
- Confidentiality by default
- Consent
- Information released to third parties
- AI – automated decisions
- Portability
- Keeping, anonymizing and destroying information
- Management and notification of incidents

Roles and responsibilities

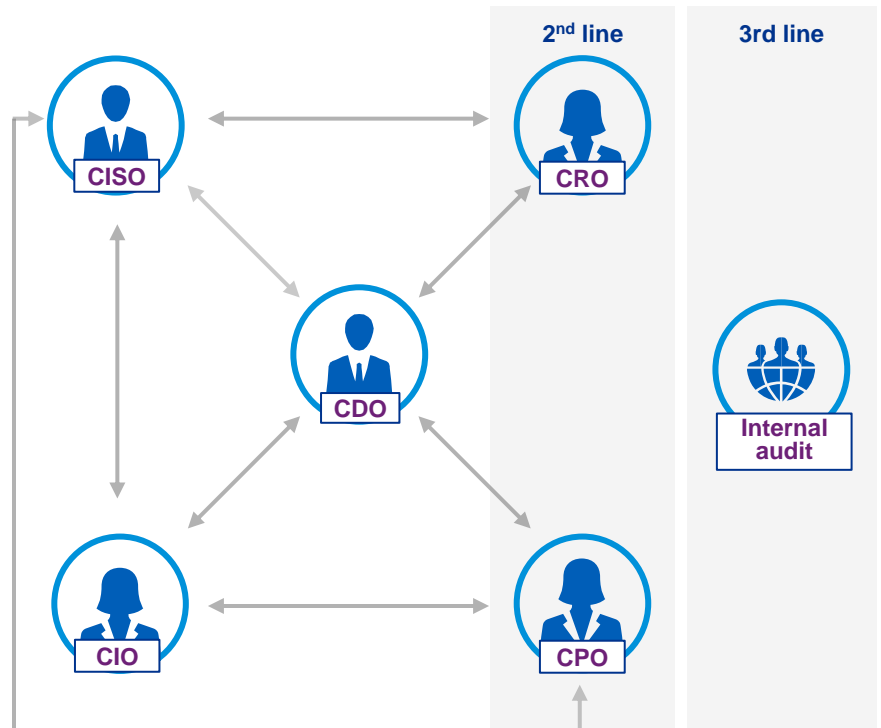
Organizations will need a well-structured approach to manage privacy risks. Now, more than ever, the roles and responsibilities for managing personal information must be clearly defined, communicated and understood.

Areas of compliance	Requirements
<p>Governance</p> <p>Roles and responsibilities</p> <p>2022</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Functions involved</p> <p>Senior management Board of directors Human resources</p> </div> <p>S.3.1 APPIPS SS. 8, 8.1 ADPBPI¹</p>	<ul style="list-style-type: none"> → Designate the person in charge of protecting people’s personal information (<i>Chief Privacy Officer “CPO”</i>) → Develop a model for delegating responsibility within the different sectors and administrative units → Determine needs and undertake the staffing process → Determine, assign and document roles and responsibilities for implementing the privacy program → Develop a matrix for assigning responsibility (e.g., RACI “<i>Responsible, Accountable, Consulted, Informed</i>”) that is tailored to the organization’s reality so as to align the CPO’s roles and responsibilities with those of other officers involved in data governance and management (CISO, CIO, CDO, CRO) as well as internal audit according to the model based on three lines of defence

Model for delegating responsibility for privacy



Stakeholder relationships




¹The obligation to designate a person in charge of document access existed prior to the Act.


Policies, processes and solutions

Given their obligations to protect people’s personal information, organizations need to document their practices, show transparency and support people in exercising their rights. Technological solutions will have to be considered to support an organization’s privacy program.

Areas of compliance	Requirements
<p>Governance</p> <p>Policies, processes, solutions</p> <p>2023</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px auto; width: fit-content;"> <p>Functions involved</p> <p>Privacy</p> <p>Legal services</p> <p>Security</p> <p>IT</p> <p>Communication</p> </div> <p>Ss. 3.2, 8, 8.2, 12.1 APPIPS Ss.. 63.3, 63.4, 65, 84 ADPBPPPI</p>	<p>→ Develop and implement policies, practices and registers for:</p> <ul style="list-style-type: none"> ○ Roles and responsibilities of stakeholders within the organization; ○ Gathering and processing PI; ○ Keeping and destroying PI; ○ Handling complaints; ○ Existing controls and security measures to ensure confidentiality (when PI is gathered using technology); ○ Detecting and managing security incidents; ○ Recording security incidents and statements/notices; ○ Methods used to de-identify and anonymize information. <p>→ Publish information on the website, using clear, precise and transparent language, regarding policies and practices for:</p> <ul style="list-style-type: none"> ○ Collecting and processing PI; ○ Keeping and destroying PI; ○ Stakeholders’ roles and responsibilities; ○ Handling complaints; ○ Existing controls and security measures to ensure confidentiality (when PI is gathered using technology). <p>→ Develop and implement effective internal processes to respond to requests for:</p> <ul style="list-style-type: none"> ○ Information (PI collected, people with access to this information, retention period, contact information for the person in charge); ○ Access and changes to the PI collected; ○ Requests to stop releasing the information or to require that it be de-indexed; ○ Explanations for automated processing mechanisms; ○ The processing of biometric data; ○ Portability; ○ Withdrawal of consent. <p>→ Establish the functional requirements, select and deploy technological solutions according to the technology architecture in place.</p>



Fact sheet – processing and assessment of privacy-related factors



PI protection policy



PI inventory/ mapping/ register




Procedure for managing confidentiality incidents



Fact sheet – positions in charge of protecting PI



Regulatory compliance controls



Employee training and awareness material

Impact assessment

The Act formalizes good practices, which consist in assessing the privacy impacts of projects that involve the use of personal information. These assessments make it possible to identify and remedy any risks while the project in question is still at the development stage, thereby reducing the risks when the project is subsequently deployed.

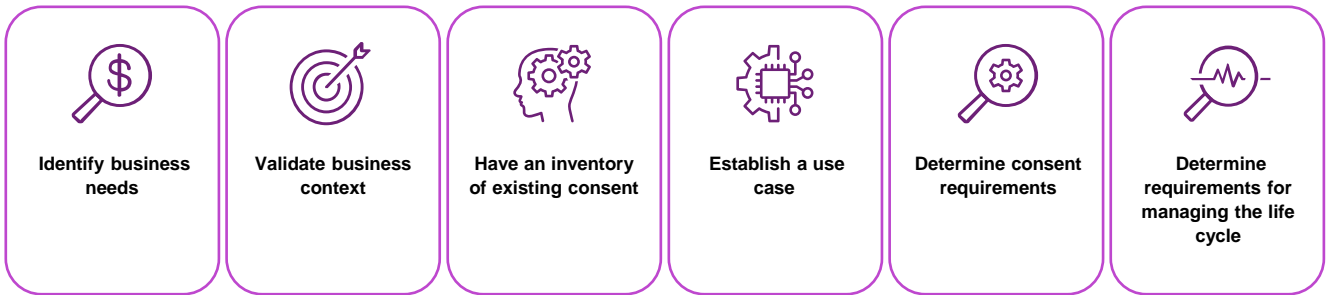
Areas of compliance	Requirements
<p>Assessment of privacy-related factors</p> <p>2023</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Functions involved</p> <p>Privacy</p> <p>Business – project office</p> <p>Data governance</p> <p>Development of solutions</p> <p>Procurement</p> <p>IT</p> </div> <p>Ss. 3.3 - 3.4, and 17 APPIPS Ss. 63.5, 70.1 ADPBPI</p>	<ul style="list-style-type: none"> → Develop and implement a process for analyzing impacts (assessment of privacy-related factors, according to the Act) which applies to: <ul style="list-style-type: none"> ○ any project involving the acquisition, development or redesign of an information system or electronic service delivery involving the use of PI; ○ PI released to third parties for research purposes; ○ PI released outside Québec. (see <i>section below on information released to suppliers/cloud solutions</i>). → Identify project management processes and specific project categories, such as: <ul style="list-style-type: none"> ○ Implementation of an ERP or HCM/ER system such as <i>SAP-Success Factors and Workday</i>; ○ Implementation of a CRM system; ○ Acquisition of a cloud solution for recruiting personnel or providing client support which requires that customer data be stored or that there be employees outside Québec; ○ Development of an API for customer data; ○ Deployment of a mobile app providing access to customer accounts. → Develop a risk assessment template with the necessary controls for the risks identified. → Establish functional requirements, select and implement technological solutions to support impact analyses.

Consent

Organizations must be transparent when seeking and managing consent to ensure compliance and incorporate these requirements in their strategy and business processes.

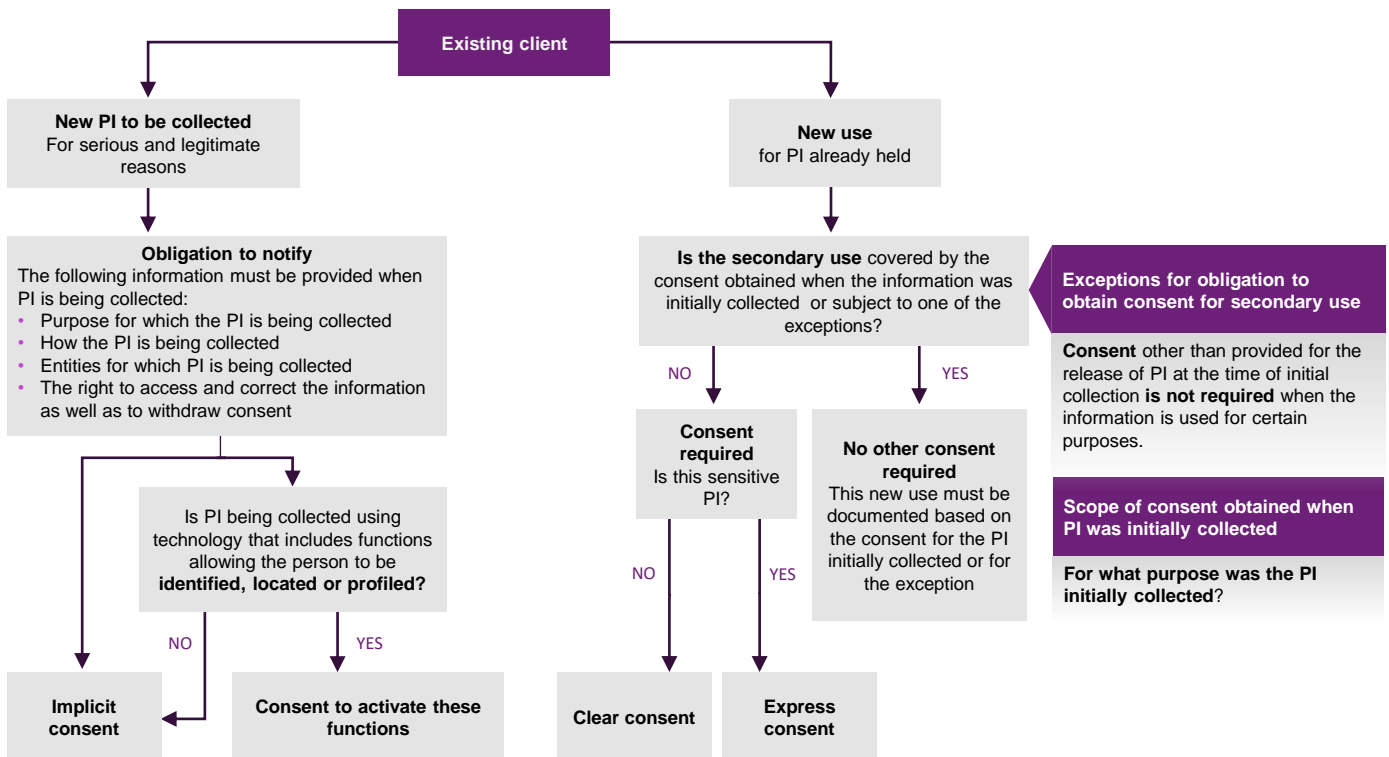
Organizations need to identify privacy compliance requirements based on business needs, the entities involved, processing activities, the targeted individuals, the context and the type of PI.

Approach for determining consent requirements:



We recommend identifying privacy compliance needs to support sectors in determining how to go about seeking and managing consent.

Sample chart to support business sectors:



Consent

Requirements and exceptions

- **Collection** - A **transparent** process that includes clear communication of the prescribed information (purpose, means used, third party recipients, person’s rights) entails an **implicit consent** regarding the use and release of the PI for the serious and legitimate reasons indicated when the information was collected.
- **Secondary uses – Consent** other than that provided when the PI was initially collected **is required** when the information is to be used for purposes other than the serious and legitimate reasons indicated when the information was initially collected or that are subject to one of the exceptions provided by the Act.
- **Exceptions – No consent** other than that provided for the communication of PI at the time of initial collection **is required** for other uses that are:
 - Consistent with the purposes for which consent was obtained;
 - Clearly for the benefit of the person to whom the information relates;
 - Necessary to prevent and detect fraud or to assess and improve security and protection measures;
 - Necessary for the supply of a product or the provision of a service requested by the individual concerned;
 - Required for study, research or statistical purposes and the PI has been de-identified.

Areas of compliance	Requirements
<div style="text-align: center;"> <p>Consent</p> <p>2023</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Functions involved</p> <p>Privacy</p> <p>Customer experience</p> <p>Business – project office</p> <p>Data governance</p> <p>Development of solutions</p> <p>IT</p> </div> <div style="margin-top: 20px;"> <p>Ss. 12, 14 APPIPS</p> <p>S. 53,1 ADPBPI</p> </div>	<ul style="list-style-type: none"> → Identify uses i) for which the organization has already obtained consent, ii) that constitute secondary uses subject to an exception (sec. 12), iii) and that require additional consent → Analyze customer journeys and communication channels to pinpoint opportunities to seek consent → Review user interfaces, tools, solutions and scenarios for obtaining consent in order to: <ul style="list-style-type: none"> ○ Seek consent, in a transparent manner, for specific purposes separately from any other information ○ Log and document the consent obtained ○ Ensure that notices of withdrawal of consent can be received and processed → Implement the processes and solutions required to consolidate the consent obtained from different sources and ensure that it is possible to validate that the consent is compatible for all other secondary uses for the PI. → Establish the functional requirements and choose the technological solutions based on the existing technological architecture → Plan the mechanism/process resulting in the renewal of consent → Establish a mechanism to seek and obtain explicit consent to use sensitive personal information → Establish ways to de-identify PI for research or statistical purposes.

Collection

A **transparent process** that consists of providing the prescribed information (purpose, means, third party recipients, person's rights) entails **implicit consent** for the PI to be used and communicated for the serious and legitimate purposes indicated at the time of collection.

Areas of compliance	Requirements
<p data-bbox="196 583 532 653">Notification at time of collection</p> <p data-bbox="326 684 402 716">2023</p> <div data-bbox="164 852 581 1140" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p data-bbox="245 867 500 898">Functions involved</p> <p data-bbox="326 926 418 957">Privacy</p> <p data-bbox="315 978 430 1010">Business</p> <p data-bbox="261 1031 488 1062">Client experience</p> <p data-bbox="358 1083 391 1115">IT</p> </div> <p data-bbox="269 1310 477 1362">Ss.. 4, 8, 8.3 APPIPS Sec. 65 ADPBPI</p>	<ul style="list-style-type: none"> <li data-bbox="618 573 1474 800">→ List the processes that involve collecting PI and identify the data and metadata to validate: <ul style="list-style-type: none"> <li data-bbox="672 627 1065 659">○ The PI that was actually collected <li data-bbox="672 667 1414 720">○ The purpose for which the PI was collected (serious and legitimate interests) <li data-bbox="672 732 1149 764">○ The PI that is required for these purposes <li data-bbox="672 772 1203 804">○ PI that is being sought for secondary purposes <li data-bbox="618 812 1474 1083">→ Review the notices and communications to include: <ul style="list-style-type: none"> <li data-bbox="672 842 1312 873">○ The purposes for which the information is being collected <li data-bbox="672 882 1154 913">○ The means used to collect the information <li data-bbox="672 921 1398 953">○ The rights to access and correct the information set out in the Act <li data-bbox="672 961 1446 1014">○ The right to withdraw consent for the release or use of the information collected <li data-bbox="672 1022 1474 1083">○ The categories of third party who will receive the PI and the possibility to release this information outside Québec, if applicable <li data-bbox="618 1092 1390 1178">→ Put in place safeguards to restrict access as well as the use and the communication of the PI for the stated purposes, in addition to control mechanisms <li data-bbox="618 1199 1365 1356">→ Put in place organizational procedures, including a register for the information being processed or a mapping of data flows to: <ul style="list-style-type: none"> <li data-bbox="672 1262 1360 1314">○ Allow individuals to exercise their rights to access and correct information and to withdraw their consent <li data-bbox="672 1323 1057 1354">○ Respond to information requests <li data-bbox="618 1365 870 1396">→ Document collection

Identification, location and profiling

When technology is used to collect PI, functionalities allowing the person concerned to be identified, located or profiled include some additional conditions, such as confidentiality by default (meaning that the functions must be activated by the person) and the obligation to notify the person.

“Profiling” means the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person’s work performance, economic situation, health status, personal preferences, interests or behaviour.

Areas of compliance	Requirements
<p>Collection of information that allows the person to be identified, located or profiled</p> <p>2023</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Functions involved</p> <p>Privacy</p> <p>Business – Project office</p> <p>Data governance</p> <p>Development of solutions</p> <p>IT</p> </div> <p>S. 8.1 APPIPS S. 65.0.1 ADPBPI</p>	<p>When information is collected involving functions allowing the person to be identified, located or profiled:</p> <ul style="list-style-type: none"> ○ These functions must be deactivated by default without any intervention on the part of the user ○ Notices and notifications must state that these functions can be used and how to activate them <p>→ This requirement applies, in particular, to the functions for sites, applications and web browsers, behavioural marketing and location cookies and tracers</p> <p>→ Review the default configurations for the systems, applications and user interfaces, including for the collection of device IDs</p> <p>→ Analyze the customer journey and communication channels to pinpoint opportunities to request that these functions be activated</p> <p>→ Modify the user interfaces to integrate notices and requests</p> <p>→ Integrate and activate functions for logging confirmation that these functions have been activated</p>

Confidentiality by default

Confidentiality by default is a key new obligation in the Act. This means that the default configuration of any technological product or service must restrict the use of personal information. It will be up to the user to voluntarily activate additional functions.

Areas of compliance	Requirements
<p>Information collected using a technological product or service</p> <p>2023</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Functions involved</p> <ul style="list-style-type: none"> Privacy Business – Project office Data governance Development of solutions Procurement IT </div> <p>S. 9.1 APPIPS S. 63.6.1 ADPBPI</p>	<ul style="list-style-type: none"> → List the technological products, services and solutions that involve collecting PI from the public: <ul style="list-style-type: none"> ○ Mobile applications and websites, including functions and web browsers or behavioural marketing cookies and tracers ○ Technological communications platforms ○ Solutions that involve accessing device IDs → Review the default configurations to provide the highest level of confidentiality, without any intervention → Settings offering users a choice must be deactivated <ul style="list-style-type: none"> ○ Can only be activated by the user → User should be free to choose to configure the confidentiality settings by opting to activate the functions that collect PI → Integrate the principle of minimizing the collection of PI and the requirements ensuring confidentiality by default in the processes for designing and developing systems and applications → Analyze the customer journey and communications channels to pinpoint opportunities for requesting that these functions be activated → Modify the user interfaces to integrate notifications and requests → Integrate and activate logging functions confirming that the functions have been activated <p>Excluded:</p> <ul style="list-style-type: none"> ○ Confidentiality settings for connection cookies are expressly excluded ○ The scope of the requirement refers to a good or service offered to the public and, therefore, does not apply to solutions implemented in a work environment – <i>However, it is important to note that the requirements pertaining to the profiling and geolocation functions referred to above apply in a work environment.</i>

Suppliers – Service providers

Organizations remain responsible for the personal information collected or provided to them, including when the PI is entrusted to third parties. It is therefore important to manage these contractual relationships properly. The Act includes specific provisions when PI is transferred outside Québec.

Areas of compliance	Requirements
<p data-bbox="180 577 548 762">Information provided to suppliers/cloud solution providers Information transferred outside Québec</p> <p data-bbox="326 787 399 821">2023</p> <div data-bbox="164 955 581 1369" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p data-bbox="248 970 500 999">Functions involved</p> <ul style="list-style-type: none"> <li data-bbox="326 1024 423 1054">Privacy <li data-bbox="289 1079 461 1108">Procurement <li data-bbox="256 1134 493 1163">Risk management <li data-bbox="261 1188 488 1218">Data governance <li data-bbox="289 1243 461 1272">IT – Business <li data-bbox="280 1297 469 1327">Legal services </div> <p data-bbox="256 1625 488 1675">Ss. 17, 18. 3 APPIPS Ss. 67.2, 70.1 ADPBPI</p>	<ul style="list-style-type: none"> <li data-bbox="618 590 1406 642">→ Review the procurement and risk management processes applicable to service providers to identify: <ul style="list-style-type: none"> <li data-bbox="695 667 1435 751">○ Projects that involve accessing or releasing PI to service providers, e.g., as part of a data migration/conversion or the integration of information systems <li data-bbox="695 772 1419 825">○ Projects that involve a migration to cloud solutions (SAAS, PAAS, IAAS) <li data-bbox="695 846 1446 909">○ Projects that involve releasing personal information outside Québec (e.g., access, storage, hosting) <li data-bbox="618 930 1459 989">→ Review the minimal contractual provisions regarding privacy (lists of minimal requirements, standard clauses, consent to the use of data), to cover: <ul style="list-style-type: none"> <li data-bbox="672 1010 1317 1039">○ Restrictions to PI that can be used or kept by the supplier <li data-bbox="672 1052 992 1081">○ Security measures applied <li data-bbox="672 1094 1105 1123">○ Notification of confidentiality incidents <li data-bbox="672 1136 1049 1165">○ Control/verification mechanisms <li data-bbox="618 1207 1406 1236">→ When the project involves providing or releasing PI outside Québec: <ul style="list-style-type: none"> <li data-bbox="672 1257 1027 1287">○ Assess the country or territory <li data-bbox="672 1299 1476 1352">○ Determine the level of sensitivity of the PI collected and the purposes for which it is to be used <li data-bbox="672 1365 1360 1394">○ Take a position as a company for the appropriate jurisdictions <li data-bbox="672 1407 1419 1488">○ Conduct an impact analysis (the Act refers to an assessment of the privacy-related factors) to determine whether the PI should be adequately protected where it is being transferred and stored <li data-bbox="618 1539 1252 1568">→ If there are any risks, agree upon mitigation measures: <ul style="list-style-type: none"> <li data-bbox="672 1589 1195 1619">○ techniques: encrypting or de-identifying the PI <li data-bbox="672 1631 1398 1684">○ organizational: restrictions for sharing the information with foreign authorities

AI - Automated decisions

Managing automated decisions regarding a person is a new aspect related to the protection of personal information. This requires detailed knowledge of the organization's decision-making processes as well as transparency and procedural guarantees that the individuals will be protected.

Areas of compliance	Requirements
<p>Automated decisions Artificial intelligence</p> <p>2023</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Functions involved</p> <p>Privacy</p> <p>Business – Project office</p> <p>Data governance</p> <p>Development of solutions</p> <p>Procurement</p> <p>IT</p> </div> <p>S. 12.1 APPIPS S. 65.2 ADPBPI</p>	<p>→ List the processes that involve the automated processing of PI to make a decision regarding employees or clients. For example:</p> <ul style="list-style-type: none"> ○ A client's ability to receive products, services or benefits based on its financial situation, risk profile or health status ○ A candidate's eligibility for employment or an employee's eligibility for promotion ○ A person's eligibility for privileges due to a status or competency profile, or a risk profile <p>→ Review the configuration of systems, applications and user interfaces to ensure that the persons concerned by the automated processing and use of PI are notified</p> <p>For example, if the processing is based on a form, this form will have to be revised to allow the person to:</p> <ul style="list-style-type: none"> ○ Ascertain, before or at the time of the decision, that the decision was based on an automated process ○ Determine which PI is used to make the decision ○ Know the reasons, factors and parameters that led to the decision ○ Correct the PI that led to the decision ○ Have the decision be reviewed by someone with the authority to change it

Retention, destruction and anonymization

Personal information should not be kept for longer than required for the purposes identified and the applicable retention period. It is possible to anonymize personal information at the end of this period to be able to continue to derive value from it. This practice must be well managed.

Areas of compliance	Requirements
<p>Retention, destruction, and anonymization data / Decommissioning a system</p> <p>2023</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Functions involved</p> <p>Privacy</p> <p>Data governance</p> <p>IT</p> </div> <p>S.23 APPIPS. S. 73 ADPBPI</p>	<ul style="list-style-type: none"> → Develop and implement a retention schedule for the PI (e.g., specific requirements for each type of PI) → Implement a mechanism to automatically and systematically destroy PI depending on retention requirements → Determine the specific levels of reidentification risk → Provide mechanisms/methods for anonymizing PI based on the risk levels identified → For all PI, determine business needs that reflect a serious and legitimate interest resulting in information being anonymized → Establish a suspension of proceedings in the event of litigation referring to the obligation to keep information

Data portability

The right to data portability will apply to personal data collected by an organization. This means that organizations will need to rely on extensive knowledge of the data collection process and the capabilities for tracing data that is held.

Areas of compliance	Requirements
<p>Data portability</p> <p>2024</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Functions involved</p> <p>Privacy</p> <p>Data governance</p> <p>Client experience</p> <p>IT</p> </div> <p>S.. 27 APPIPS S.. 84 ADPBPI</p>	<ul style="list-style-type: none"> → Validate the ability to identify the PI collected from the person (compared to PI that has been generated or inferred) → Put in place data tracing capabilities to map data flows → Determine functional requirements, select and deploy technological solutions to ensure that requests can be traced and processed → Develop APIs to automate processes for sending and receiving communication requests → Ensure the inter-operability of the solutions deployed with the sectoral standards being developed → Review the conversion/client onboarding processes to integrate portability features into the customer journey

Management and notification of incidents

Managing incidents is crucial in the protection of PI. Due to the potentially public nature of incidents and the resulting impacts on both the individuals and the organization, detection, processing and monitoring capabilities are required. Clear processes, employee training, the creation of a crisis unit and periodic practice play a key role in managing incidents.

Areas of compliance	Requirements
<p>Confidentiality incident</p> <p>2022</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Functions involved</p> <p>Privacy</p> <p>Security</p> <p>Legal services</p> <p>Communication</p> <p>IT</p> <p>Finance</p> </div>	<ul style="list-style-type: none"> → Implement a process for managing confidentiality incidents and privacy breaches, documenting this process in a plan (the “plan”). <ul style="list-style-type: none"> ○ The scope of the plan must include: the unauthorized access, use or release of PI, the loss or any other failure to protect such PI, which could include: <ul style="list-style-type: none"> ▪ Sending file attachments to the wrong recipients ▪ Unauthorized use of identifiers ▪ Loss of medium on which PI was stored ▪ Unauthorized access in a telework situation ▪ Network intrusions ▪ Exfiltration of data by internal or external hackers ▪ Ransomware-type attacks ○ Identify the stakeholders concerned: <ul style="list-style-type: none"> ▪ Members of management ▪ Legal counsel ▪ Board of directors ○ Establish a RACI chart (roles and responsibilities) and an escalation process to: <ul style="list-style-type: none"> ▪ Manage the investigation and resolution of the incident ▪ Manage internal and external communications ▪ Assess the risks of harm resulting from the incident ▪ Establish a notification process (who, when, how) to notify the following parties in the event of a breach: <ul style="list-style-type: none"> • Commission d'accès à l'information (CAI) • The individuals affected by the security incident • Third parties concerned, including clients responsible for processing PI → The plan includes one or more decision trees or criteria to establish guidelines for internal and public communications → Develop and present mandatory training for employees when they are hired, with annual refresher training (e.g., impact analyses, detecting and managing incidents, applying organizational procedures) → Conducting confidentiality incidents simulation annually to test and strengthen response capabilities, scenario-based management and the injection sequence corresponding to risk scenarios → Incorporate requirements for the notification process for breaches into the confidentiality policy, including relevant privacy-related information → Create and maintain a register of confidentiality incidents

Ss. 3.5 and 3.8 APPIPS
S. 63.3 ADPBPI

PENALTIES

Any failures or violations of the obligations set out in the Act will be subject to significant administrative penalties or penal sanctions.

We expect that the *Commission d'accès à l'information* will take a proactive stance, as was the case when the GDPR came into effect. Compliance gaps could give rise to significant monetary penalties, confidentiality breaches for clients, a loss of client trust and a devastating reputational risk.



Infractions	Failure	Maximum penalty
Administrative* S. 90.1 ss APPIPS	→ Fails to report a confidentiality incident.	Natural person: \$50,000 Legal person: \$10,000,000 or 2% of sales Prescription period: 2 years from the date of offence
	→ Collects, uses, communicates, keeps or destroys information in contravention of the APPIPS.	
	→ Fails to take the necessary security measures to protect PI.	
	→ Fails to meet the requirements for automated decisions.	
	→ Third party action.	
	→ Fails to meet the transparency obligations.	
Penal Ss. 91, 92 and ss APPIPS Ss. 158-159 ADPBPI	→ Fails to report a confidentiality incident.	Natural person: \$100,000 Legal person: \$25,000,000 or 4% of sales (whichever is greater) Repeat offence: double the penalty Prescription period: 5 years from the date of offence
	→ Collects, uses, communicates, keeps or destroys information in contravention of the APPIPS.	
	→ Fails to take the necessary security measures to protect PI.	
	→ Asks another credit assessment officer for PI after being notified of a security freeze.	
	→ Attempts to re-identify a person using de-identified or anonymized information without the authorization of the persons holding the information.	
	→ Impedes the progress of an inquiry or an inspection by the CAI.	
	→ Threatens to take reprisals against a person for filing a complaint or cooperating with the CAI.	
	→ Fails to comply with an order by the CAI.	
→ Fails to produce the requested documents within the time period specified by the CAI.		

*Administrative infractions also apply to private sector bodies.

Detailed framework for protecting PI



—

Questions asked by private and public organizations

Do I have a clear understanding of the personal information that is collected and processed within or on behalf of the organization?

When, how, by whom and for what purpose?

Where is this information stored and for how long?

Do I have trust in the organization's ability to detect and effectively manage a confidentiality incident?

Do we confirm and monitor suppliers for confidentiality and security compliance?

How will the new requirements impact our operations?

What are the organization's compliance risks?





Why
choose
KPMG?

**A Canadian leader
for data
management
and privacy.**

KPMG has completed a broad range of privacy, governance and data management projects across a variety of industries.

We recognize the challenges arising from the coming into force of the Act and have the experience and resources required to assist you in identifying gaps and deficiencies in your current situation and successfully completing your compliance project.

“We stand out due to our approach based on respect for privacy ‘from the development stage and by default’, which seeks to integrate and automate the principles of privacy in developing processes, products or services that require the use of personal information.”

JEAN-FRANÇOIS DE RICO

KPMG Partner, Advisory

Data Privacy – Technology Risk
Management – Cybersecurity

Checklist

September 2022

- Person in charge of privacy protection
- Third persons (research and business transactions)
- Confidentiality incidents
- Biometrics
- Whistleblower protection
- Obligation to cooperate with the CAI

September 2023

- Policies and procedures
- Assessment of privacy-related factors
- Confidentiality by default
- De-identification
- Anonymization
- Third parties and information disclosed outside Québec
- Notice of confidentiality
- Transparency (in general)
- Consent
- Purpose restrictions
- Collection restrictions
- Keeping and destroying information
- Deleting information
- Automated decisions and profiling

September 2024

- Portability

This is a good opportunity to take back control of your data and leverage this strategic asset.

KPMG's approach

A holistic, pragmatic approach that is based on complementary skills and collaboration with data professionals:

- **Cyber security**
- **Data privacy**
- **Data management and governance**
- **Automation**
- **Document management**
- **Digital transformation**
- **Identity and access management**
- **Client experience**
- **Change management**

We prefer to take a holistic approach based on complementary experience and proven collaboration by our professionals

Our team includes seasoned professionals working in complementary areas. They are committed to excellence and often work together so that clients can benefit from a multidisciplinary approach and well thought-out solutions.

KPMG can leverage its international network of privacy professionals to serve you, when necessary.

Our team

Privacy protection



Jean-François De Rico
Lead Partner,
Data Privacy
KPMG in Canada

jderico@kpmg.ca
418 577-3442



François Senécal
Senior Manager,
Data Privacy
KPMG in Canada



Raphaël Jauvin
Senior manager,
Data Privacy
KPMG in Canada



Abigail Dubiniecki
Manager,
Data Privacy
KPMG in Canada



Virginie Bernier
Senior Consultant,
Data Privacy
KPMG in Canada



Jean-Luc Nicholson
Senior consultant,
Data Privacy
KPMG in Canada



Camélia Jamali
Consultant,
Data Privacy
KPMG in Canada



Sylvia Kingsmill
Global Cyber Privacy Leader
KPMG in Canada

Governance and data management



Catherine Nadeau
Senior Manager,
Data Governance
KPMG in Canada

cnadeau@kpmg.ca
514 840-5350



Emmanuel Thorens
Senior Manager,
Data Governance
KPMG in Canada



Alexandre Longeval
Manager,
Data Governance
KPMG in Canada



Cynthia Viau-Mainville
Manager,
Document Management
KPMG in Canada

Digital transformation



Patricia Boisclair
Senior Manager,
Digital Transformation and Strategy
KPMG in Canada



Jenna Yee
Manager,
Digital Transformation and Strategy
KPMG in Canada

Cyber Security



Yassir Bellout
Partner,
Cyber Security
KPMG in Canada



Claudio Francavilla
Senior Manager,
Cyber Security
KPMG in Canada

Client experience



Derek Derouin
Senior Manager,
Client Experience
KPMG in Canada



Guillaume Baur
Manager,
Client Experience
KPMG in Canada



Vincent De Bruille
Consultant,
Client Experience
KPMG in Canada

Change management



Julie Grenier
Manager,
Change Management
KPMG in Canada



[kpmg.ca](https://www.kpmg.ca)

© 2022 KPMG LLP, an Ontario limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.